REMARKS

The enclosed is responsive to the Final Office Action mailed on April 30, 2008. At the time the Final Office Action was mailed, claims 29-36 and 67-82 were pending. By way of the present response, Applicant has amended no claims; cancelled no claims; and added no claims. As such, claims 29-36 and 67-82 are now pending. Applicants respectfully request reconsideration of the present application and the allowance of all claims now presented.

Examiner Interview Summary

Applicant thanks the Examiner for his courtesy, time, and effort advanced during the examiner interview on June 27, 2008. During the interview, the Livingston and Morkel references were discussed in relation to Applicant's claimed invention, and the Examiner indicated that the current rejection would likely be withdrawn. In addition, the Examiner indicated the possibility that Keller, Arthur M., "An Independent, Reliable, Distributed, and Secure Spam Opt-Out Registry", University of California at Santa Cruz (hereinafter "Keller I") and Keller, et al., "An Opt-Out Registry for Spam Email", University of California at Santa Cruz (hereinafter "Keller II") may be used in a future rejection.

The Keller References

As previously described, during the interview, the Examiner raised the possibility of using the Keller references (Keller I and/or Keller II) as prior art references in a future rejection. Applicant submitted the Keller references in an Information Disclosure Statement filed on 10/21/03. Unfortunately, neither of the Keller references includes a date. Applicant does not admit that either of the Keller references qualifies as prior art (see cover letter to the 10/21/03 IDS stating that submission is not a admission that the references are material to patentability), and

Applicant reserves the right to swear behind or establish that Keller I and Keller II do not predate Applicant's provisional filing date (e.g., with the filing of a 37 CFR § 1.132 declaration). Second, assuming arguendo that Keller I and/or Keller II does qualify as prior art, Applicant respectfully submits that Keller I and/or Keller II, alone and/or in combination with Livingston and/or Morkel (if such combination is proper – see below), does not teach or suggest the required limitations of Applicants claims.

Claim Rejections – 35 U.S.C. § 103

Claims 29-36 and 67-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ben Livingston , Possible Modifications to Washington, anti-spam law, Internet Newsgroup, January 31, 2002, (hereinafter "Livingston") in view of Morkel, U.S. Patent No. 7,007,068 B2 (hereinafter "Morkel").

Claims 80-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Livingston" in view of "Morkel" and further in view of Lu, U.S. Patent No. 7,174,453 (hereinafter "Lu").

Not Obvious to Combine Livingston and Morkel

Applicant respectfully submits that it would not have been obvious for one of ordinary skill in the art at the time of the invention to combine Livingston and Morkel as proposed by the Office Action.

Livingston describes two separate concepts. The first concept (described in 6 sentences) discusses a Washington anti-spam law and the attempt of an individual (Heckel) to overturn that anti-spam law (paragraphs 1-3). Heckel was a spammer who did not want to comply with the Washington anti-spam law (the law is briefly described in paragraph 1). The Washington anti-spam law only applies to Washington residents. Since Heckel did not want to comply with the Washington law, he could not send offending emails to Washington residents (but presumably could send those emails to residents of other states). Since an email address by itself does not indicate the location of the email address owner, Heckel argued that a "spammer must contact the domain

name registrant for every email address on their list" in order to determine which email addresses belonged to Washington residents (paragraph 3). For example, if the spammer wanted to transmit emails to the email addresses joe.smith@hotmail.com, bill.smith@yahoo.com, etc., the spammer would have to contact hotmail.com and yahoo.com to determine if joe.smith and bill.smith are Washington residents. It should be noted that this concept does not suggest a 'do not email list'. In other words, this concept does not suggest that the domain name registrant has a 'do not email list'.

The second concept is a 1 sentence comment about a "do not email list". The full sentence is as follows: "I feel that a "do not email" list would work well; unfortunately, such a list could be seriously abused" (paragraph 4). Thus, Livingston does not teach a "do not email" list; rather Livingston only has a 1 sentence comment, in passing, about such a list and states that the list would have problems and does not provide any guidance or suggestion on how to solve those problems. Thus, Livingston did not perceive there was a solution to the potential of serious abuse of a "do not email" list.

Applicant respectfully submits that Livingston does not combine the two separate concepts. Livingston would have combined the two concepts if he believed they were combinable. Assuming arguendo that the two concepts are combinable, the intended purpose of Livingston is to create a "do not email" list to prevent sending spam to Washington residents.

Morkel describes a system that allows an email sender to control the time and frequency of sending updates of personal information (contact information) to select recipients and to securely protect the access of that personal information so that the personal information is received only by the selected recipients (Col 2, lines 4-10). Thus, Morkel describes a system for facilitating transmission of personal contact information in a secure fashion. The personal contact information of a user is stored on a server (Col 4, lines 12-18; server 17). The sender typically hashes a recipient's email address and transmits this to the server (see Morkel, Arrow 1 in Figure 1A), and the server associates this hash with the personal contact information (Col 3, lines 2-8). A sender transmits an email to a recipient which includes an indication that contact information is available to that recipient (Col 2 lines 31-35; Arrow 4 in Figure 1A). The recipient receives the email and, after determining it wants the contact

information, accesses the server (e.g., by clinking on a URL link in the received email) where the access further includes the recipient transmitting either a hashed version of the recipient's email address, or the raw unhashed recipient's email address (the server then hashes the recipient's email address) (Col 6, lines 40-49; Figure 1A, arrow 5). The server compares the stored hash of the recipient's email address (transmitted by the sender) and the hash of the recipient's email address provided by the intended recipient. If the two hashes match, the server has verified that this particular recipient may receive the personal information and forwards the personal information to that recipient (Col 2, lines 43-46; Col 6, lines 45-49; Figure 1A, arrow 6).

The Office Action alleges that Livingston describes substantially all of the limitations in the claims except it "fails to expressly use of hashed email addresses" (Office Action, page 3). Thus, the proposed combination of Livingston and Morkel would have the system of facilitating transmission of personal contact information in a secure fashion of Morkel incorporated into the "do not email" list comment of Livingston. However, Applicant respectfully submits that one of ordinary skill in the art would not have combined Livingston and Morkel for at least the following reasons.

First, Applicant respectfully submits that in the first concept described in Livingston, there is no need for any hashing scheme, let alone the hashing scheme described in Morkel. For example, in the first concept as described in Livingston, the spammer (Heckel) has email addresses it wants to contact (e.g., joe.smith@hotmail.com). Thus, the spammer knows that the domain name registrant for those email addresses (e.g., hotmail.com) presumably include those email addresses (e.g., joe.smith@hotmail.com). Thus, the fact that the email address joe.smith@hotmail.com exists at the domain name registrant hotmail.com is not a secret to the spammer (Heckel) and is not a secret to the domain name registrant (hotmail.com). Thus, there is no suggestion or motivation for that email address to be hashed in any fashion, since both parties (the spammer (Heckel) and the domain name registrant (hotmail.com)) are already aware of the underlying content (e.g., joe.smith@hotmail.com). In contrast, in the claimed invention, neither party has knowledge of what the other party has on its list. Thus, in Applicant's claimed invention, prior to comparison, neither party knows what is on the other parties list.

Second, Applicant respectfully submits this proposed combination renders Livingston unsatisfactory for its intended purpose.[1] As stated previously, the intended purpose of Livingston is to create a "do not email" list to prevent sending spam to Washington residents. The proposed combination includes modifying Livingston by introducing a sender, a server, and a recipient. In the proposed combination, the sender hashes an email address of a recipient and transmits the hashed email address to the server, which stores the hashed email address. The sender then transmits an email to that recipient. The recipient typically hashes its email address and transmits the hashed email address to the server. The server compares the stored hashed email address with the hashed email address received from the recipient.

However, it is unclear to Applicant what the Office Action suggests the combination teaches or suggests as occurring as a result of the comparison. As described previously, Morkel describes that if the hashes match, the server transmits personal contact information to the recipient, and the recipient stores and presumably at transmits an email to the client at some point. If the hashes do not match, the server does not transmit personal contact information to the recipient, and the recipient presumably does nothing. However, a "do not email" list, as commented by Livingston, presumably includes email addresses that **do not** want to be contacted. One possible interpretation is that if the hashes match (e.g., the hashed email address of the recipient matches a stored hashed email address), the server transmits an email to the recipient. However, this interpretation renders Livingston's intended purpose to create "do not email" to prevent sending spam to Washington residents unsatisfactory. For example, presumably the combination describes the server storing a list of hashed email addresses that **do not** want to receive email. If the hashes match (and thus the email address is on the do not contact list) and the server **transits an email** to that email address, then the intended purpose of Livingston is rendered unsatisfactory (i.e., emails are transmitted to email addresses that did not to receive emails). Another possible interpretation is that if the hashes do not match, the server does not transmit

[1] MPEP $ 2143.01(V), The Proposed Modification Cannot Render the Prior Art Unsatisfactory For Its Intended Purpose, "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification."

an email to the recipient. However, this interpretation renders Livingston's intended purpose to create a "do not email" list unsatisfactory. For example, presumably the combination describes the server storing a list of hashed email addresses that **do not** want to receive email (thus, presumably email addresses that are **not** on the list are presumably safe to email).

Third, the proposed combination would describe the sender transmitting an email message to the intended recipient regardless of any comparison of the hash values, or any other spam prevention schemes. For example, Morkel describes the sender transmitting an email to the intended recipient **prior** to the server comparing hash values (see Figure 1A, arrow 4). Thus, it is illogical, and thus evidence that it is not obvious to combine, to perform the hashing techniques of Morkel (presumably for anti-spam purposes) **after** email addresses are transmitted to intended recipients.

Therefore, for at least these reasons, Applicant respectfully submits that the independent claims 29, 67, 71, and 79 are allowable. Applicant respectfully submits that the dependant claims 30-36, 68-70, 72-78, and 80-82 are allowable for at least the reason that they are dependent on an allowable independent claim.

Combination does not teach or suggest required limitations

Applicant respectfully submits that the combination of Livingston and Morkel does not teach or suggest the required limitations of Applicant's claims.

Claim 29

Applicant respectfully submits that the combination of Livingston and Morkel does not teach or suggest the required limitations of Claim 29. In addition, Applicant respectfully submits that Keller I and/or Keller II does not teach or suggest, alone and/or in combination with Livingston and/or Morkel, the required limitations of Claim 29. Claim 29 recites (emphasis added):

29. A computer implemented method comprising:

collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;

applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list entries, wherein the one-way hashing scheme is intended to conceal the do-not-email list entries from an intended recipient;

transferring the set of one or more hashed do-not-email list entries to **a master do-not-email list server** configured to store the set of one or more hashed do-not-email list entries without revealing the email address corresponding to each of the hashed do-not-email list entries;

requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a **client** do-not-email list **on a client machine**;

causing a **client** email entry to be hashed using the same one-way hashing scheme to create a **hashed client email entry**;

comparing the hashed **client** email entry to the hashed do-not-email list entries **on the client do-not-email list** to determine whether the hashed **client** email entry appears on the **client** do-not-email list; and

transmitting at least one email to the email address that corresponds to the hashed **client** email entry upon determining that the hashed **client** email entry does not appear on the **client** do-not-email list.

Thus, claim 29 requires a master do-not-email list **server** storing one or more hashed do-no-email list entries (e.g., a master do-not-email list), a **client machine** storing a **client do-not-email list** that is created or updated by **requesting from** the master do-not-email list **server** at least one hashed do-not-email list entry (e.g., a separate client do-not-email list on a client machine), a hashing of an email address already in the client's possession (a client email entry) to create a hashed client email entry, and comparing the hashed client email entry to the hashed do-not-email list entries on the client do-not-email list to determine whether the hashed client email entry appears on the client do-not-email list, and transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list.

First, the proposed combination does not teach or suggest the limitation "requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list **on a client machine**" as required by claim 29 (emphasis added).

Firstly, the proposed combination does not teach or suggest requesting a hashed do-not-email list entry from the do-not-email list server. The proposed combination only describes transferring a hashed email address to the server (Morkel, Col 2, lines 37-38). In addition, the proposed combination describes the server storing "a hash of the recipient's e-mail address received from the client" and the "server then forwards the e-mail with the transaction ID to the recipient" (Morkel, Col 2, lines 35-40). Thus, the proposed combination describes the server transmitting an email (unhashed) to a recipient, but does not describe the server transmitting a hashed email list entry as alleged by the Office Action. Furthermore, the proposed combination does not describe requesting a hashed do-not-email list entry from the master do-not-email list server to create or update a **client** do-not-email list on a **client machine** as alleged by the Office Action. Therefore, Applicant respectfully submits that the combination does not teach or suggest "requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list **on a client machine**" as alleged by the Office Action, and respectfully requests the rejection be clarified to address this limitation with regard to the combination (e.g., other than simply pointing to Applicant's claim language) if the rejection is maintained.

Second, the proposed combination does not teach or suggest the limitation "comparing the hashed client email entry to the hashed do-not-email list entries **on the client do-not-email list** to determine whether the hashed client email entry appears on the client do-not-email list" as required by claim 29 (emphasis added). While the proposed combination describes the **server** comparing a stored hash of a recipient's email address with a computed hash of the recipient's email address, and if the hashes match transmitting contact information to the recipient, the proposed combination does not describe comparing any hashed email entries to other hashed do-not-email list entries on the client do-not-email list. Simply put, the proposed combination describes only the **server** comparing hashed email entries (Morkel, Col 2 lines 39-46; Col 2 lines 54-58). In contrast, claim 29 requires comparison against the client do-not-email list, which is on the **client machine**.

Third, the proposed combination does not teach or suggest the limitation "transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list" as required by claim 29 (emphasis added). To illustrate, in Applicant's claimed invention, after receiving the results of the comparison, the client transmits at least an email to an email address in the client's list whose corresponding encrypted entry did not match any of the encrypted entries on the do not contact list. Thus, the email addresses whose corresponding encrypted entries in the client's list did not match the encrypted entries on the do not contact list are safe for the client to email (e.g., those email addresses are not on the do not contact list). In contrast, in the proposed combination, if the there is no match, the server does not transmit personal contact information to the recipient, and the recipient presumably does nothing. Thus, in the proposed combination, emails are not transmitted as a result of determining there is not a match between hashes. Furthermore, in the proposed combination, the sender transmits an email to the recipient regardless of the comparison performed by the server (the sender transmits the email to the recipient prior to the comparison) (see Morkel, Figure 1A, arrow 4). In addition, in the proposed combination, if there is no match, the server does not transmit personal contact information to the recipient (see Morkel, Col 6, lines 46-49) and therefore presumably the recipient does not transmit an email. Therefore, for at least these reasons, Applicant respectfully submits the proposed combination does not teach or suggest "transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list." as required by claim 29 (emphasis added).

Furthermore, the above limitations are not obvious in view of the combination for at least the following two reasons. First, Applicant's claimed invention allows significant advantages as compared to the combination. To illustrate Applicant's claimed invention and by way of example and not limitation, there are two lists each controlled by different parties (e.g., one list controlled by the government and the other list controlled by an email marketer). The content of the two lists is not shared between the parties, but the lists are compared to each other to discover which entries from the second list (e.g., email

marketer's list) are also on the first list (e.g., the government's list). The lists are email addresses controlled by the two different parties. The email addresses are confidential, and the comparison is for the purposes of not transmitting email to matching entries. It is accomplished through hashing each entry on both lists; tracking unhashed entries for the second list (e.g., the email marketer's list) and the correspondence between the unhashed entries and their counterpart hashed values; comparing the hashed entries of the two lists; and then correlating the results back to the original unhashed second list of email addresses. Each email address determined to be on the first list (e.g., the government's list) will not receive an email (e.g., the email marketer does not send email to the email address determined to be on the government's list).

To say it a different way, by way of example and not limitation, an email marketer has one list of email addresses that the email marketer wants to contact for marketing purposes and another party, in our example the government, has their own list of email addresses that make up a do-not-contact list. The email marketer is not allowed to contact email addresses that choose to opt out of email marketing (i.e., the email addresses on the government's list) so the email marketer desires to check the entries on the government's list to determine if the email marketer should remove an entry from their list. However, the government does not want to share their list of unhashed email addresses that do not wish to be contacted as this information can be very valuable to unscrupulous email marketers (e.g., if the list of unhashed email addresses were compromised, then unscrupulous email marketers could contact the email addresses of people that do not wish to be contacted). Additionally, the email marketer also does not want to share their list of unhashed email addresses because this information is also very valuable to the email marketer and they do not want this list to be public for fear of unscrupulous email marketers (e.g., for the same reasons as above). Therefore, in Applicants' claimed invention a one-way hashing scheme is used by both entities (government and email marketer) such that each entity will have a list containing hashed entries. These two lists can then be compared and matches determined. Thus, with Applicants' claimed invention, for example, the underlying content of the lists (i.e., the email addresses represented by the hashed values on both lists) can be compared (e.g., by comparing the hashed entries on both lists) (in order for the email marketer to determine

which email address shall not be contacted) without either party sharing their list of unhashed email addresses. In other words, the government does not trust sharing its unhashed email addresses with the email marketer; and similarly the email marketer does not trust sharing its unhashed email addresses with the government. However, since it is nearly mathematically impossible for an unhashed email address to be determined solely from examining a one way hashed email address, each party (e.g., the government and the email marketer) is willing to share one way hashed email addresses with each other for comparison purposes.

Secondly, as recognized by Livingston, "a do-not email list would well; unfortunately, such list could be seriously abused" (Livingston, Paragraph 4, emphasis added). Thus, Livingston did not perceive there was a solution to the potential of serious abuse of a "do not email" list.

Thus, Applicant respectfully submits that the combination of Livingston, Morkel, and/or Keller I and/or Keller II, does not teach or suggest the required limitations of claim 29. Thus, Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

In addition, Applicant respectfully submits that the dependant claims 30-36 depend on claim 29 and are allowable for at least the same reason.

Claims 67 and 71

Applicant respectfully submits that the combination of Livingston and Morkel does not teach or suggest the required limitations of Claim 67 or Claim 71. In addition, Applicant respectfully submits that Keller I and/or Keller II does not teach or suggest, alone and/or in combination with Livingston and/or Morkel, the required limitations of Claims 67 or 71. Claim 67 recites (emphasis added):

> 67. A computer implemented method to identify email addresses registered on a **do not contact list** that are in a **client's list** without revealing the email addresses on the **do not contact list** or the **client's list** comprising:
>
> the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address,

wherein the entries are encrypted in a way that it is intended that an intended recipient cannot decrypt the entries;

the client transmitting over a network said plurality of encrypted entries from the client's list **to a service** for comparison to encrypted entries of the do not contact list, wherein the encrypted entries of the do not contact list were formed by encrypting information, including at least an email address, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs to be identified;

the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list; and

the client transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list.

Thus, claim 67 requires **two** lists: a do not contact list and a client's list, each including a plurality of email addresses. The client encrypts (e.g., hashes) entries on its list. Entries of the do not contact list are also hashed. The client transmits its encrypted entries to a service for comparison to encrypted entries of the do not contact list (thus, the service performs the comparison). The client receives the result of the comparison which indicates which of its encrypted entries match the encrypted entries on the do not contact list, and the client transmits an email to an email address whose encrypted entry did not match any of the encrypted entries on the do not contact list.

First, the proposed combination of Livingston and Morkel does not teach or suggest the limitation "the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list" as required by claim 67 (emphasis added). Applicant respectfully submits that the proposed combination does not teach or suggest the above limitation. The proposed combination describes that the server transmits personal contact information to the recipient if the hashes match (e.g., see Morkel, Col 2, lines 47-58). However, the proposed combination does not teach or suggest the client receiving results of the comparison. In addition, the proposed combination does not teach or suggest the client receiving results "wherein the results

of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list" as required by claim 67. In other words, in the proposed combination, the server compares hashes to determine if the recipient may receive the personal contact information (the comparison is performed to verify the identify of the recipient). Therefore, Applicant respectfully submits the proposed combination does not teach or suggest "the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list" as required by claim 67 (emphasis added).

Secondly, the proposed combination does not teach or suggest the limitation "the client transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list" as required by claim 67 (emphasis added). It should be noted that this limitation was not addressed by the Office Action (see Office Action pages 7 and 8). If this rejection is maintained, Applicant respectfully requests that this part of the limitation be addressed. Nevertheless, Applicant respectfully submits that the proposed combination does not teach or suggest the above limitation. To illustrate, in Applicant's claimed invention, after receiving the results of the comparison, the client transmits at least an email to an email address in the client's list whose corresponding encrypted entry did not match any of the encrypted entries on the do not contact list. Thus, the email addresses whose corresponding encrypted entries in the client's list did not match the encrypted entries on the do not contact list are safe for the client to email (e.g., those email addresses are not on the do not contact list). In contrast, in the proposed combination, if the there is no match, the server does not transmit personal contact information to the recipient, and the recipient presumably does nothing. Furthermore, in the proposed combination, the sender transmits an email to the recipient regardless of the comparison performed by the server (the sender transmits the email to the recipient prior to the comparison) (see Morkel, Figure 1A, arrow 4). In addition, in the proposed combination, if there is no match, the server does not transmit personal

contact information to the recipient (see Morkel, Col 6, lines 46-49) and therefore presumably the recipient does not transmit an email. Therefore, for at least these reasons, Applicant respectfully submits the proposed combination does not teach or suggest "the client transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list" as required by claim 67 (emphasis added).

Thus, certain limitations have not been addressed by the Office Action, certain limitations that were addressed by the Office Action are not taught or suggested by the proposed combination, and these limitations are not obvious in view of the combination for at least the reasons as discussed with reference to claim 67.

Thus, for at least the above reasons, Applicant respectfully submits that the combination of Livingston, Morkel, and/or Keller I and/or Keller II does not teach or suggest the required limitations of claim 67. Thus, Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

In addition, Applicant respectfully submits that the dependant claims 68-70 depend on claim 67 and are allowable for at least the same reason.

Regarding claim 71, Applicant respectfully submits that claim 71 includes similar limitations as claim 67 with the addition that "the encrypted entries of the do - not-contact list were formed by encrypting information, including at least an email address that belongs to a minor" (claim 71, emphasis added).

Thus, Applicant respectfully submits that the combination of Livingston, Morkel, and/or Keller I and/or Keller II does not teach or suggest the required limitations in claim 71 for at least the same reasons as claim 67.

Applicant respectfully submits that the dependant claims 72-78 depend on claim 71 and are allowable for at least the same reason.

Claim 79

Applicant respectfully submits that the combination of Livingston and Morkel does not teach or suggest the required limitations of Claim 79. In addition, Applicant respectfully submits that Keller I and/or Keller II does not teach or suggest, alone and/or

in combination with Livingston and/or Morkel, the required limitations of Claim79. Claim 79 recites (emphasis added):

> Claim 79. A computer implemented method to identify email addresses registered on a do-not-contact list without revealing the email addresses on the do-not-contact list comprising:
>
> a client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each encrypted entry includes at least an email address that does not wish to be contacted, wherein the entries are encrypted in a way that it is intended that an intended recipient cannot decrypt the entries;
>
> the client causing a comparison of said plurality of encrypted entries from the client's list to a plurality of encrypted entries of a master do-not-contact list, wherein the encrypted entries of the master do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the master do-not-contact list represents that the underlying email address needs to be identified;
>
> the client receiving results of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not-contact list, and the results do not reveal the email addresses on the master do-not-contact list;
>
> the client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list; and the client transmitting at least an email to the at least one email address that corresponds to the removed entry.

First, Applicant assumes that claim 79 was summarily rejected by the Office Action as reciting the limitations of claims 29 and 67 and therefore rejected for the same reasons as claims 29 and 67 (Office Action, page 9).[2] However, Applicant respectfully submits that claim 79 includes distinct and different limitations than those in claims 29 or 67. For example, unlike claim 29 or claim 67, claim 79 requires "a client encrypting at least certain entries on the client's list to create a plurality of encrypted entries, where each encrypted entry includes at least an email address that does not wish to be contacted" (emphasis added). Thus, in claim 79, the **client's** list

[2] The Office Action states "***Regarding Claim 79,*** it recites the limitations of claims 29 and 67, and therefore it is" (Office Action, page 9). For this response, Applicant assumes that the Office Action meant to additionally state that claim 79 is rejected for the same reasons as claims 29 and 67.

includes unencrypted email addresses that do not wish to be contacted (e.g., email addresses previously determined to be on a master do not contact list) and these entries are then encrypted. These encrypted entries of the client are compared with encrypted entries of the master do not contact list for the purpose of verifying whether the entries of the client are still on the master do not contact list (i.e., whether the unencrypted email addresses still do not wish to be contacted). As another example, unlike claim 29 or claim 67, claim 79 requires "the client updating the client's list with the results to **remove** the at least one of the entries on the client's list that is not on the master do-not-contact list" (emphasis added). Applicant respectfully requests clarification of the rejection if the rejection is to be maintained.

Second, Applicant respectfully submits that the combination of Livingston and Morkel does not teach or suggest the limitation "the client receiving results of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not-contact list, and the results do not reveal the email addresses on the master do-not-contact list" as required by claim 79 (emphasis added). The proposed combination describes if the hashes match, the server transmits personal contact information to the recipient (Morkel, Col 2, lines 47-58). However, the proposed combination does not teach or suggest the client receiving results of the comparison. In other words, in the proposed combination, the server is not comparing the hashes for the client, but rather is comparing a recipient's email address hash to determine if the recipient may receive the personal contact information (i.e., the comparison is performed to verify the recipient's identity). Therefore, Applicant respectfully submits the proposed combination does not teach or suggest "the client receiving results of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not-contact list, and the results do not reveal the email addresses on the master do-not-contact list" as required by claim 79 (emphasis added).

Third, Applicant respectfully submits that the combination of Livingston and Morkel does not teach or suggest the limitation "the client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list; and the client transmitting at least an email to the at least one email address that corresponds to the removed entry" as required by claim 79

(emphasis added). The proposed combination does not teach or suggest that the client removes an entry from its list (its own do not contact list) that is not on the master do not contact list. The proposed combination only describes, as a result of the comparison, transmitting personal information to the recipient if the hashes match, and presumably not transmitting the personal information to the recipient if the hashes do not match.

Thus, for at least the above reasons, Applicant respectfully submits that the combination of Morkel, Livingston, and/or Russell, does not teach or suggest the required limitations of claim 79. Thus, Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

Claims 80-82 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Livingston in view of Morkel and further in view of Lu, U.S. Patent No. 7,174,453 (hereinafter "Lu"). Applicant respectfully submits that the dependant claims 80-82 depend on allowable indepdent claim 79 and are allowable for at least the same reason.

CONCLUSION

Applicant respectfully submits that all rejections have been overcome and that all pending claims are in condition for allowance. If there are any additional charges, please charge them to our Deposit Account Number 02-2666. If a telephone conference would facilitate the prosecution of this application, Examiner is invited to contact Daniel M. De Vos at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: June 30, 2008

/Daniel M. De Vos/
Daniel M. De Vos
Reg. No. 37,813

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300